# SR-680374472 SG500: Problemi di vulnerabilità con SSL

## Riepilogo

L'analisi Nessus ha rilevato delle vulnerabilità nelle suite di cifratura supportate.

## Data identificazione

18 mag 2016

## Data risoluzione

17 febbraio 2017

## Prodotti interessati

| | |
|---|---|
| Serie SG500 | 1.4.5.02 |

## Descrizione problema

La scansione di Nessus mostra un algoritmo hash debole, una vulnerabilità SSL. Il servizio remoto utilizza una catena di certificati SSL firmata utilizzando un algoritmo di hash debole dal punto di vista crittografico (ad esempio MD2, MD4, MD5 o SHA1). Questi algoritmi di firma sono noti per essere vulnerabili agli attacchi di collisione. Un utente non autorizzato può sfruttare questa funzionalità per generare un altro certificato con la stessa firma digitale, consentendo a un utente non autorizzato di mascherare il servizio interessato.

## Risoluzione

Il problema deve essere risolto quando si esegue l'aggiornamento all'ultima versione del firmware 1.4.7.06.